PATENT
81942.0015
Express Mail Label No. EL 713 626 455 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Kiyoko KATAYANAGI et al.

Serial No: Not assigned

Filed: May 21, 2001

For: ENCRYPTION METHOD, DECRYPTION METHOD, CRYPTOGRAPHIC COMMUNICATION METHOD, CRYPTOGRAPHIC COMMUNICATION SYSTEM, MEMORY PRODUCT AND DATA SIGNAL EMBODIED IN CARRIER WAVE

Art Unit: Not assigned

Examiner: Not assigned

TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed herewith are certified copies of Japanese patent application Nos. 2000-153358 filed May 24, 2000 and 2000-307822 filed October 6, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: May 21, 2001

By: _____
Michael Crapenhoft
Registration No. 37,115
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　５月２４日

出願番号
Application Number: 特願２０００－１５３３５８

願人
Applicant (s): 村田機械株式会社
笠原　正雄

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　３月２３日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１－３０２３０００

【書類名】　特許願

【整理番号】　21218

【提出日】　平成12年 5月24日

【あて先】　特許庁長官殿

【国際特許分類】　G09C 1/00

H04K 1/00

【発明の名称】　暗号化方法，復号方法，暗号通信システム及び記録媒体

【請求項の数】　12

【発明者】

【住所又は居所】　滋賀県大津市仰木の里東８丁目７－１２

【氏名】　片柳　磨子

【発明者】

【住所又は居所】　京都府京都市伏見区竹田向代町１３６番地　村田機械株式会社　本社工場内

【氏名】　村上　恭通

【発明者】

【住所又は居所】　大阪府箕面市粟生外院４丁目１５番３号

【氏名】　笠原　正雄

【特許出願人】

【識別番号】　000006297

【氏名又は名称】　村田機械株式会社

【代表者】　村田　純一

【特許出願人】

【識別番号】　597008636

【氏名又は名称】　笠原　正雄

【代理人】

【識別番号】　100078868

【弁理士】

【氏名又は名称】　河野　登夫

【電話番号】　06-6944-4141

【選任した復代理人】

【識別番号】　100114557

【弁理士】

【氏名又は名称】　河野　英仁

【電話番号】　06-6944-4141

【手数料の表示】

【予納台帳番号】　001889

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9805283

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号化方法，復号方法，暗号通信システム及び記録媒体

【特許請求の範囲】

【請求項１】　平文から暗号文を得る暗号化方法において、暗号化すべき平文をＫ分割してなるＫ個の成分を有する第１ベクトルにＲ個の任意の乱数を成分とする第２ベクトルを加えた（Ｋ＋Ｒ）個の成分を有する第３ベクトルと、整数d_i（$1 \leqq i \leqq K+R$）を用いて（Ｋ＋Ｒ）個の各成分D_iが$D_i = d / d_i$（但し、$d = d_1\ d_2 \cdots d_{K+R}$（任意の２つの整数$d_i$，$d_j$は互いに素））に設定された第４ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項２】　平文から暗号文を得る暗号化方法において、暗号化すべき平文をＫ分割してなるＫ個の成分を有する第１ベクトルにＲ個の任意の乱数を成分とする第２ベクトルを加えた（Ｋ＋Ｒ）個の成分を有する第３ベクトルと、整数d_i（$1 \leqq i \leqq K+R$）及び乱数v_iを用いて（Ｋ＋Ｒ）個の各成分V_iが$V_i = (d / d_i) \cdot v_i$（但し、$d = d_1\ d_2 \cdots d_{K+R}$（任意の２つの整数$d_i$，$d_j$は互いに素））に設定された第４ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項３】　平文から暗号文を得る暗号化方法において、暗号化すべき平文をＫ分割してなるＫ個の成分を有する第１ベクトルにＲ個の任意の乱数を成分とする第２ベクトルを加えた（Ｋ＋Ｒ）個の成分を有する第３ベクトルと、複数組の整数d_i（$1 \leqq i \leqq K+R$）を用いて各組毎に（Ｋ＋Ｒ）個の各成分D_iが$D_i = d / d_i$（但し、$d = d_1\ d_2 \cdots d_{K+R}$（任意の２つの整数$d_i$，$d_j$は互いに素））に設定された複数の第４ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項４】　平文から暗号文を得る暗号化方法において、暗号化すべき平文をＫ分割してなるＫ個の成分を有する第１ベクトルにＲ個の任意の乱数を成分とする第２ベクトルを加えた（Ｋ＋Ｒ）個の成分を有する第３ベクトルと、複数組の整数d_i（$1 \leqq i \leqq K+R$）及び乱数v_iを用いて各組毎に（Ｋ＋Ｒ）個の各成分V_iが$V_i = (d / d_i) \cdot v_i$（但し、$d = d_1\ d_2 \cdots d_{K+R}$（任意の２つの整数$d_i$，$d_j$は互いに素））に設定された複数の第４ベクトルとを用い

て暗号文を得ることを特徴とする暗号化方法。

【請求項５】　前記第３ベクトルの各成分と、前記第４ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分とによる積和演算により暗号文を得るようにした請求項１～４の何れかに記載の暗号化方法。

【請求項６】　平文から暗号文を得る暗号化方法において、

暗号化すべき平文をＫ分割してなる平文ベクトル$m=(m_1, m_2, \cdots, m_K)$に任意の乱数を成分とする疑似平文ベクトル$m'=(m_{K+1}', m_{K+2}', \cdots, m_{K+R}')$を加えた拡大平文ベクトル$m''=(m_1'', m_2'', \cdots, m_{K+R}'')$と、整数$d_i$（$1 \leqq i \leqq K+R$）を用いて$D_i = d/d_i$（但し、$d=d_1 d_2 \cdots d_{K+R}$（任意の２つの整数$d_i$，$d_j$は互いに素））に設定された基数ベクトル$D=(D_1, D_2, \cdots, D_{K+R})$とを用いて、前記平文を暗号文に変換することとし、

（Ｋ＋Ｒ）個の乱数v_iを生成して、式（ａ）により変換基数積V_iを導くステップと、

$$V_i = D_i \ v_i \qquad \cdots (a)$$

式（ｂ）により定義される積和平文Ｍに対して、Ｍ＜Ｐを満たす素数Ｐを生成するステップと、

$$M = m_1'' V_1 + m_2'' V_2 + \cdots + m_{K+R}'' V_{K+R} \qquad \cdots (b)$$

ｗ＜Ｐを満たす乱数ｗを定め、式（ｃ）により公開鍵ベクトル$c=(c_1, c_2, \cdots, c_{K+R})$を求めるステップと、

$$c_i \equiv w V_i \pmod{P} \qquad \cdots (c)$$

拡大平文ベクトルm''と公開鍵ベクトルｃとの内積により、式（ｄ）に示す暗号文Ｃを作成するステップと

$$C = m_1'' c_1 + m_2'' c_2 + \cdots + m_{K+R}'' c_{K+R} \qquad \cdots (d)$$

を有することを特徴とする暗号化方法。

【請求項７】　請求項６にて得られた暗号文を復号する復号方法であって、前記暗号文Ｃに対して、積和平文Ｍを式（ｅ）のようにして求めるステップと、

$$M \equiv w^{-1} C \pmod{P} \qquad \cdots (e)$$

積和平文Mに対して、平文ベクトルmを式（ｆ）のようにして復号するステップと

$$m_i \equiv MV_i^{-1} \pmod{d_i} \quad \cdots (f)$$

を有することを特徴とする復号方法。

【請求項８】　平文から暗号文を得る暗号化方法において、

暗号化すべき平文をＫ分割してなる平文ベクトルm＝（m_1，m_2，…，m_K）に任意の乱数を成分とする疑似平文ベクトルm′＝（m_{K+1}'，m_{K+2}'，…，m_{K+R}'）を加えた拡大平文ベクトルm″＝（m_1''，m_2''，…，m_{K+R}''）と、素数Ｐ，Ｑに関して２組の整数$d_i^{(P)}$，$d_i^{(Q)}$，（$1 \leqq i \leqq K+R$）を用いて$D_i^{(P)} = d^{(P)} / d_i^{(P)}$（但し、$d^{(P)} = d_1^{(P)} d_2^{(P)} \cdots d_{K+R}^{(P)}$（任意の２つの整数$d_i^{(P)}$，$d_j^{(P)}$は互いに素）），$D_i^{(Q)} = d^{(Q)} / d_i^{(Q)}$（但し、$d^{(Q)} = d_1^{(Q)} d_2^{(Q)} \cdots d_{K+R}^{(Q)}$（任意の２つの整数$d_i^{(Q)}$，$d_j^{(Q)}$は互いに素））に設定された２つの基数ベクトル$D^{(P)}$，$D^{(Q)}$とを用いて、前記平文を暗号文に変換することとし、

２組の（Ｋ＋Ｒ）個の乱数$v_i^{(P)}$，$v_i^{(Q)}$を生成して、式（ｇ），（ｈ）により変換基数積$V_i^{(P)}$，$V_i^{(Q)}$を導くステップと、

$$V_i^{(P)} = D_i^{(P)} v_i^{(P)} \quad \cdots (g)$$

$$V_i^{(Q)} = D_i^{(Q)} v_i^{(Q)} \quad \cdots (h)$$

中国人の剰余定理を用いて、Ｐ，Ｑによる余りが夫々$V_i^{(P)}$，$V_i^{(Q)}$となるような最小の変換基数積$V_i^{(N)}$（Ｎ＝ＰＱ）を求めるステップと、

変換基数積$V_i^{(N)}$と拡大平文ベクトルm″とを用いて、式（ｉ）により積和平文Mを定義するステップと、

$$M = m_1'' V_1^{(N)} + m_2'' V_2^{(N)} + \cdots + m_{K+R}'' V_{K+R}^{(N)} \quad \cdots (i)$$

w＜Ｎを満たす乱数wを定め、式（ｊ）により公開鍵ベクトルc＝（c_1，c_2，…，c_{K+R}）を求めるステップと、

$$c_i \equiv wV_i \pmod{N} \quad \cdots (j)$$

拡大平文ベクトルm″と公開鍵ベクトルｃとの内積により、式（ｋ）に示す暗号文Ｃを作成するステップと

$$C = m_1 \prime\prime c_1 + m_2 \prime\prime c_2 + \cdots + m_{K+R} \prime\prime c_{K+R} \quad \cdots (k)$$

を有することを特徴とする暗号化方法。

【請求項９】　請求項８にて得られた暗号文を復号する復号方法であって、前記暗号文Ｃに対して、積和平文Ｍを式（１）のようにして求めるステップと

$$M \equiv w^{-1} C \pmod{N} \quad \cdots (1)$$

Ｐ，Ｑにおける積和平文M_P，M_Qを式（ｍ），（ｎ）のようにして求めるステップと、

$$M_P \equiv M \pmod{P} \quad \cdots (m)$$

$$M_Q \equiv M \pmod{Q} \quad \cdots (n)$$

式（ｏ），（ｐ）によって（$m_i^{(P)}$，$m_i^{(Q)}$）を求め、中国人の剰余定理を適用することにより、式（ｑ）から平文ベクトルｍを復号するステップと

【数１】

$$m_i^{(P)} \equiv M_P V_i^{(P)-1} \pmod{d_i^{(P)}} \cdots (o)$$

$$m_i^{(Q)} \equiv M_Q V_i^{(Q)-1} \pmod{d_i^{(Q)}} \cdots (p)$$

$$m_i \equiv \begin{cases} m_i^{(P)} \pmod{d_i^{(P)}} \\ m_i^{(Q)} \pmod{d_i^{(Q)}} \end{cases} \cdots (q)$$

を有することを特徴とする復号方法。

【請求項１０】　複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項１～６または８の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文から元の平文を復号する復号器とを備えることを特徴とする暗号通信システム。

【請求項１１】　コンピュータに、平文から積和型の暗号文を得させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体にお

いて、暗号化すべき平文をＫ分割したＫ個の成分を有する平文ベクトルにＲ個の任意の乱数を成分とする疑似平文ベクトルを加えて（Ｋ＋Ｒ）個の成分を有する拡大平文ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、整数d_i（$1 \leqq i \leqq K+R$）及び乱数v_iを用いて（Ｋ＋Ｒ）個の各成分V_iが$V_i = (d / d_i) \cdot v_i$（但し、$d = d_1\ d_2 \cdots d_{K+R}$（任意の２つの数$d_i$，$d_j$は互いに素））に設定された基数ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、前記拡大平文ベクトルの各成分と前記基数ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分との積和演算により暗号文を得ることをコンピュータに実行させるプログラムコード手段とを有することを特徴とする記録媒体。

【請求項１２】　コンピュータに、平文から積和型の暗号文を得させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文をＫ分割したＫ個の成分を有する平文ベクトルにＲ個の任意の乱数を成分とする疑似平文ベクトルを加えて（Ｋ＋Ｒ）個の成分を有する拡大平文ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、複数組の整数d_i（$1 \leqq i \leqq K+R$）及び乱数v_iを用いて各組毎に（Ｋ＋Ｒ）個の成分V_iが$V_i = (d / d_i) \cdot v_i$（但し、$d = d_1\ d_2 \cdots d_{K+R}$（任意の２つの数$d_i$，$d_j$は互いに素））に設定された複数の基数ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、前記拡大平文ベクトルの各成分と前記複数の基数ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分との積和演算により暗号文を得ることをコンピュータに実行させるプログラムコード手段とを有することを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、公開鍵を用いて平文を暗号文に変換する公開鍵暗号系に関し、特に、積和型暗号に関する。

【０００２】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【０００４】

暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者とが同じ共通鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を元に平文に復号する。

【０００５】

これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異なっており、公開されている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵に

よって変換された暗号文は秘密鍵でのみ復号することができる。

【０００６】

公開鍵暗号系の１つの方式として、積和型暗号方式が知られている。これは、送信者である一方のエンティティ側で平文をＫ分割した平文ベクトルｍ＝（m_1，m_2，・・・，m_K）と公開鍵である基数ベクトルｃ＝（c_1，c_2，・・・，c_K）とを用いて、暗号文Ｃ＝m_1 c_1 ＋m_2 c_2 ＋・・・＋m_K c_K を作成し、受信者である他方のエンティティ側でその暗号文Ｃを秘密鍵を用いて平文ベクトルｍに復号して元の平文を得る暗号化方式である。

【０００７】

このような整数環上の演算を利用した積和型暗号に関して、新規な方式及び攻撃法が次々に提案されているが、特に、多くの情報を短時間で処理できるように高速復号可能な暗号化・復号の手法の開発が望まれている。そこで、本発明者等は、中国人の剰余定理を用いることにより、高速な並列復号処理を可能とした積和型暗号における暗号化方法及び復号方法を提案している（特開2000－89669 号）。この暗号化方法は、基数ベクトルｃの成分c_i（ｉ＝１，２，・・・，Ｋ）を、互いに素なＫ個の整数d_iを用いてD_i＝ｄ／d_i（但し、ｄ＝d_1 d_2・・・d_K）に設定した基数D_iを基にモジュラ変換したもの、または、互いに素なＫ個の整数d_i，乱数v_iを用いてD_i＝（ｄ／d_i）v_iに設定した基数D_iを基にモジュラ変換したものにすることを特徴としている。このようにして、中国人の剰余定理を用いて並列に復号するので、高速な復号を行うことができる。

【０００８】

【発明が解決しようとする課題】

しかしながら、この方式では、公開鍵の数を非常に大きくしない限り低密度であるので、ＬＬＬ（Lenstra-Lenstra-Lovasz）アルゴリズムを用いて公開鍵と暗号文とから直接平文を求める低密度攻撃に弱い場合があるという問題があり、安全性の面での更なる改良が望まれている。

【０００９】

本発明は斯かる事情に鑑みてなされたものであり、上記従来例を改良して低密

度攻撃に強く、安全性を向上できる暗号化方法及び復号方法、この暗号化方法を用いる暗号通信システム、並びに、この暗号化方法の動作プログラムを記録した記録媒体を提供することを目的とする。

【００１０】

【課題を解決するための手段】

請求項１に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文をＫ分割してなるＫ個の成分を有する第１ベクトルにＲ個の任意の乱数を成分とする第２ベクトルを加えた（Ｋ＋Ｒ）個の成分を有する第３ベクトルと、整数d_i（$1 \leqq i \leqq K+R$）を用いて（Ｋ＋Ｒ）個の各成分D_iが$D_i = d / d_i$（但し、$d = d_1\ d_2 \cdots d_{K+R}$（任意の２つの整数$d_i$，$d_j$は互いに素））に設定された第４ベクトルとを用いて暗号文を得ることを特徴とする。

【００１１】

請求項２に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文をＫ分割してなるＫ個の成分を有する第１ベクトルにＲ個の任意の乱数を成分とする第２ベクトルを加えた（Ｋ＋Ｒ）個の成分を有する第３ベクトルと、整数d_i（$1 \leqq i \leqq K+R$）及び乱数v_iを用いて（Ｋ＋Ｒ）個の各成分V_iが$V_i = (d / d_i) \cdot v_i$（但し、$d = d_1\ d_2 \cdots d_{K+R}$（任意の２つの整数$d_i$，$d_j$は互いに素））に設定された第４ベクトルとを用いて暗号文を得ることを特徴とする。

【００１２】

請求項３に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文をＫ分割してなるＫ個の成分を有する第１ベクトルにＲ個の任意の乱数を成分とする第２ベクトルを加えた（Ｋ＋Ｒ）個の成分を有する第３ベクトルと、複数組の整数d_i（$1 \leqq i \leqq K+R$）を用いて各組毎に（Ｋ＋Ｒ）個の各成分D_iが$D_i = d / d_i$（但し、$d = d_1\ d_2 \cdots d_{K+R}$（任意の２つの整数$d_i$，$d_j$は互いに素））に設定された複数の第４ベクトルとを用いて暗号文を得ることを特徴とする。

【００１３】

請求項４に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗

号化すべき平文をＫ分割してなるＫ個の成分を有する第１ベクトルにＲ個の任意の乱数を成分とする第２ベクトルを加えた（Ｋ＋Ｒ）個の成分を有する第３ベクトルと、複数組の整数d_i（$1 \leqq i \leqq K+R$）及び乱数v_iを用いて各組毎に（Ｋ＋Ｒ）個の各成分V_iが$V_i = (d / d_i) \cdot v_i$（但し、$d = d_1\ d_2 \cdots d_{K+R}$（任意の２つの整数$d_i$，$d_j$は互いに素））に設定された複数の第４ベクトルとを用いて暗号文を得ることを特徴とする。

【００１４】

請求項５に係る暗号化方法は、請求項１～４の何れかにおいて、前記第３ベクトルの各成分と、前記第４ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分とによる積和演算により暗号文を得るようにしたことを特徴とする。

【００１５】

請求項６に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文をＫ分割してなる平文ベクトル$m = (m_1, m_2, \cdots, m_K)$に任意の乱数を成分とする疑似平文ベクトル$m' = (m_{K+1}', m_{K+2}', \cdots, m_{K+R}')$を加えた拡大平文ベクトル$m'' = (m_1'', m_2'', \cdots, m_{K+R}'')$と、整数$d_i$（$1 \leqq i \leqq K+R$）を用いて$D_i = d / d_i$（但し、$d = d_1\ d_2 \cdots d_{K+R}$（任意の２つの整数$d_i$，$d_j$は互いに素））に設定された基数ベクトル$D = (D_1, D_2, \cdots, D_{K+R})$とを用いて、前記平文を暗号文に変換することとし、

（Ｋ＋Ｒ）個の乱数v_iを生成して、式（ａ）により変換基数積V_iを導くステップと、

$$V_i = D_i\ v_i \qquad \cdots (a)$$

式（ｂ）により定義される積和平文Ｍに対して、Ｍ＜Ｐを満たす素数Ｐを生成するステップと、

$$M = m_1''\ V_1 + m_2''\ V_2 + \cdots + m_{K+R}''\ V_{K+R} \qquad \cdots (b)$$

ｗ＜Ｐを満たす乱数ｗを定め、式（ｃ）により公開鍵ベクトル$c = (c_1, c_2, \cdots, c_{K+R})$を求めるステップと、

$$c_i \equiv w V_i \pmod{P} \qquad \cdots (c)$$

拡大平文ベクトルm''と公開鍵ベクトルｃとの内積により、式（ｄ）に示す暗

号文Ｃを作成するステップと

$$C = m_1'' c_1 + m_2'' c_2 + \cdots + m_{K+R}'' c_{K+R} \quad \cdots (d)$$

を有することを特徴とする。

【００１６】

請求項７に係る復号方法は、請求項６にて得られた暗号文を復号する復号方法であって、

前記暗号文Ｃに対して、積和平文Ｍを式（ｅ）のようにして求めるステップと、

$$M \equiv w^{-1} C \pmod{P} \quad \cdots (e)$$

積和平文Ｍに対して、平文ベクトルｍを式（ｆ）のようにして復号するステップと

$$m_i \equiv M V_i^{-1} \pmod{d_i} \quad \cdots (f)$$

を有することを特徴とする。

【００１７】

請求項８に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文をＫ分割してなる平文ベクトル$m = (m_1, m_2, \cdots, m_K)$に任意の乱数を成分とする疑似平文ベクトル$m' = (m_{K+1}', m_{K+2}', \cdots, m_{K+R}')$を加えた拡大平文ベクトル$m'' = (m_1'', m_2'', \cdots, m_{K+R}'')$と、素数Ｐ，Ｑに関して２組の整数$d_i^{(P)}$，$d_i^{(Q)}$，（$1 \leqq i \leqq K+R$）を用いて$D_i^{(P)} = d^{(P)} / d_i^{(P)}$（但し、$d^{(P)} = d_1^{(P)} d_2^{(P)} \cdots d_{K+R}^{(P)}$）（任意の２つの整数$d_i^{(P)}$，$d_j^{(P)}$は互いに素）），$D_i^{(Q)} = d^{(Q)} / d_i^{(Q)}$（但し、$d^{(Q)} = d_1^{(Q)} d_2^{(Q)} \cdots d_{K+R}^{(Q)}$（任意の２つの整数$d_i^{(Q)}$，$d_j^{(Q)}$は互いに素））に設定された２つの基数ベクトル$D^{(P)}$，$D^{(Q)}$とを用いて、前記平文を暗号文に変換することとし、

２組の（Ｋ＋Ｒ）個の乱数$v_i^{(P)}$，$v_i^{(Q)}$を生成して、式（ｇ），（ｈ）により変換基数積$V_i^{(P)}$，$V_i^{(Q)}$を導くステップと、

$$V_i^{(P)} = D_i^{(P)} v_i^{(P)} \quad \cdots (g)$$

$$V_i^{(Q)} = D_i^{(Q)} v_i^{(Q)} \quad \cdots (h)$$

中国人の剰余定理を用いて、Ｐ，Ｑによる余りが夫々$V_i^{(P)}$，$V_i^{(Q)}$とな

るような最小の変換基数積$V_i^{(N)}$（N＝PQ）を求めるステップと、

変換基数積$V_i^{(N)}$と拡大平文ベクトルm″とを用いて、式（i）により積和平文Mを定義するステップと、

$$M=m_1'' V_1^{(N)}+m_2'' V_2^{(N)}+\cdots+m_{K+R}'' V_{K+R}^{(N)} \quad \cdots(i)$$

w＜Nを満たす乱数wを定め、式（j）により公開鍵ベクトルc＝（c_1，c_2，…，c_{K+R}）を求めるステップと、

$$c_i \equiv w V_i \pmod N \quad \cdots(j)$$

拡大平文ベクトルm″と公開鍵ベクトルcとの内積により、式（k）に示す暗号文Cを作成するステップと

$$C=m_1'' c_1+m_2'' c_2+\cdots+m_{K+R}'' c_{K+R} \quad \cdots(k)$$

を有することを特徴とする。

【００１８】

請求項９に係る復号方法は、請求項８にて得られた暗号文を復号する復号方法であって、

前記暗号文Cに対して、積和平文Mを式（l）のようにして求めるステップと、

$$M \equiv w^{-1} C \pmod N \quad \cdots(l)$$

P，Qにおける積和平文M_P，M_Qを式（m），（n）のようにして求めるステップと、

$$M_P \equiv M \pmod P \quad \cdots(m)$$

$$M_Q \equiv M \pmod Q \quad \cdots(n)$$

式（o），（p）によって（$m_i^{(P)}$，$m_i^{(Q)}$）を求め、中国人の剰余定理を適用することにより、式（q）から平文ベクトルmを復号するステップと

【００１９】

【数２】

$$m_i^{(P)} \equiv M_P V_i^{(P)-1} \pmod{d_i^{(P)}} \quad \cdots (o)$$

$$m_i^{(Q)} \equiv M_Q V_i^{(Q)-1} \pmod{d_i^{(Q)}} \quad \cdots (p)$$

$$m_i \equiv \begin{cases} m_i^{(P)} \pmod{d_i^{(P)}} \\ m_i^{(Q)} \pmod{d_i^{(Q)}} \end{cases} \quad \cdots (q)$$

【００２０】

を有することを特徴とする。

【００２１】

請求項１０に係る暗号通信システムは、複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項１～６または８の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文から元の平文を復号する復号器とを備えることを特徴とする。

【００２２】

請求項１１に係る記録媒体は、コンピュータに、平文から積和型の暗号文を得させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文をＫ分割したＫ個の成分を有する平文ベクトルにＲ個の任意の乱数を成分とする疑似平文ベクトルを加えて（Ｋ＋Ｒ）個の成分を有する拡大平文ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、整数d_i（$1 \leqq i \leqq K+R$）及び乱数v_iを用いて（Ｋ＋Ｒ）個の各成分V_iが$V_i = (d / d_i) \cdot v_i$（但し、$d = d_1\ d_2 \cdots d_{K+R}$（任意の２つの数$d_i$，$d_j$は互いに素））に設定された基数ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、前記拡大平文ベクトルの各成分と前記基数ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分との積和演算により暗号文を得ることをコンピュータに実行させるプログラムコード手段

とを有することを特徴とする。

【００２３】

請求項１２に係る記録媒体は、コンピュータに、平文から積和型の暗号文を得させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文をＫ分割したＫ個の成分を有する平文ベクトルにＲ個の任意の乱数を成分とする疑似平文ベクトルを加えて（Ｋ＋Ｒ）個の成分を有する拡大平文ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、複数組の整数d_i（$1 \leqq i \leqq K+R$）及び乱数v_iを用いて各組毎に（Ｋ＋Ｒ）個の成分V_iが$V_i = (d / d_i) \cdot v_i$（但し、$d = d_1 d_2 \cdots d_{K+R}$（任意の２つの数$d_i$，$d_j$は互いに素））に設定された複数の基数ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、前記拡大平文ベクトルの各成分と前記複数の基数ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分との積和演算により暗号文を得ることをコンピュータに実行させるプログラムコード手段とを有することを特徴とする。

【００２４】

本発明では、平文に冗長性を持たせる、言い換えると平文を退化させて暗号文を作成する。即ち、暗号化すべき平文を分割してなる第１ベクトル（平文ベクトル）及び特に暗号化を必要としない乱数成分からなる第２ベクトル（疑似平文ベクトル）を合わせた第３ベクトル（拡大平文ベクトル）と、各成分を$D_i = d / d_i$または$V_i = (d / d_i) \cdot v_i$に設した第４ベクトル（基数ベクトル）とを用いて暗号文を作成する。具体的には、第３ベクトル（拡大平文ベクトル）の各成分と、第４ベクトル（基数ベクトル）を基に、モジュラ変換した公開鍵ベクトルの各成分との積和演算によって暗号文を構成する。よって、暗号文の密度が高くなり、１つの暗号文に対して非常に多くの復号方法が存在するので、ＬＬＬアルゴリズムに基づく低密度攻撃は非常に困難となる。この結果、安全性が向上する。

【００２５】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図１は、本発明による暗号化方法をエンティティａ，ｂ間の情報通信に利用した状態を示す模式図である。図１の例では、一方のエンティティａが、暗号化器１にて平文ｘを暗号文Ｃに暗号化し、通信路３を介してその暗号文Ｃを他方のエンティティｂへ送信し、エンティティｂが、復号器２にてその暗号文Ｃを元の平文ｘに復号する場合を示している。

【００２６】

（第１実施の形態）

秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：$\{d_i\}$，$\{d_i'\}$，$\{v_i\}$，Ｐ，ｗ

・公開鍵：$\{c_i\}$

【００２７】

ｅ＞ｅ′として、正規基数d_i及び退化基数d_i'は、夫々下記（１），（２）を満たす基数と定義する。

【００２８】

【数３】

$$d_i = 2^e + \delta_i \quad (1 \ll \delta_i \ll 2^e) \cdots (1)$$

$$d_i' = 2^{e'} + \delta_i' \quad (1 \ll \delta_i' \ll 2^{e'}) \cdots (2)$$

【００２９】

（Ｋ＋Ｒ）個の互いに素な数からなる基数を定める。但し、そのうちのｉ∈Ｉに対応するＫ個を正規基数、ｉ∈Ｉ′に対応するＲ個を退化基数とする。ここで、Ｉ，Ｉ′は何れもインデックス集合であり、Ｉ＝｛１，２，…，Ｋ｝，Ｉ′＝｛Ｋ＋１，Ｋ＋２，…，Ｋ＋Ｒ｝とし、Ｉ″＝Ｉ∪Ｉ′とする。なお、本明細書では、特に断らない限り、ｉ∈Ｉ″である。次に、基数積D_iを下記（３）に従って求める。

【００３０】

【数４】

$$D_i = \begin{cases} \dfrac{d_1 \cdots d_K d_{K+1}' \cdots d_{K+R}'}{d_i} & (i \in I) \\ \dfrac{d_1 \cdots d_K d_{K+1}' \cdots d_{K+R}'}{d_i'} & (i \in I') \end{cases} \quad \cdots (3)$$

【００３１】

また、（Ｋ＋Ｒ）個の乱数｛v_i｝を生成し、変換基数積V_iを下記（４）により導く。

$$V_i = D_i \ v_i \qquad \cdots (4)$$

【００３２】

エンティティａ側で、エンティティｂへ暗号化して送信すべき平文ｘをＫ分割して、各成分がｅ（ビット）である平文ベクトルｍ＝（m_1，m_2，…，m_K）を得る。また、エンティティｂへ特に送信する必要がない各成分がｅ（ビット）の乱数からなる疑似平文ベクトルｍ′＝（m_{K+1}，m_{K+2}，…，m_{K+R}）を得る。例えば、エンティティｂへ特に送信する必要がない平文（冗長文）をＲ分割して、この疑似平文ベクトルｍ′を得ることができる。これらの平文ベクトルｍと疑似平文ベクトルｍ′とを結合して、（Ｋ＋Ｒ）個の成分を有する拡大平文ベクトルｍ″＝（m_1″，m_2″，…，m_{K+R}″）を得る。ここで、この拡大平文ベクトルｍ″の各成分は、下記（５）のように定義される。

【００３３】

【数５】

$$m_i'' = \begin{cases} m_i & (i \in I) \\ m_i' & (i \in I') \end{cases} \quad \cdots (5)$$

【００３４】

積和平文Ｍを，拡大平文ベクトルｍ″と変換基数積V_iとを用いて、下記（６

）のように定義する。

$$M=m_1'' V_1+m_2'' V_2+\cdots+m_{K+R}'' V_{K+R} \quad \cdots(6)$$

【００３５】

任意の拡大平文ベクトルm″に対して、M＜Pを満たす素数Pを生成して法とする。素数Pより小さい乱数wを定め、下記（７）に従って、下記（８）に示すような公開鍵ベクトルcを導いて公開する。

$$c_i \equiv w V_i \pmod{P} \quad \cdots(7)$$

$$\text{ベクトル}c=(c_1, c_2, \cdots, c_{K+R}) \quad \cdots(8)$$

【００３６】

エンティティａ側で、拡大平文ベクトルm″と公開鍵ベクトルcとの内積を下記（９）のように求めて、暗号文Cを得る。作成された暗号文Cは通信路３を介してエンティティａからエンティティｂへ送信される。

$$C=m_1'' c_1+m_2'' c_2+\cdots+m_{K+R}'' c_{K+R} \quad \cdots(9)$$

【００３７】

エンティティｂ側では、以下のようにして復号処理が行われる。

暗号文Cから積和平文Mは、下記（10）のようにして求めることができる。

$$M\equiv w^{-1}C \pmod{P} \quad \cdots(10)$$

【００３８】

拡大平文ベクトルm″のうち、正規基数に対応するインデックス、即ち、i∈Iに関しては、下記（11）が成立して、平文ベクトルmを復号することができる。

$$m_i \equiv M V_i^{-1} \pmod{d_i} \quad \cdots(11)$$

【００３９】

なお、退化基数に対応するインデックス、即ち、i∈I′に関しては、復号する必要がない。また、上記（11）と同様に下記（12）に従って復号しようとしても、退化の影響によりビット数に関して下記（13）の関係があるので、疑似平文ベクトルm′を正しく復号することはできない。

$$m_i'' \equiv M V_i^{-1} \pmod{d_i'} \quad \cdots(12)$$

$$m_i' > d_i' > m_i'' \quad \cdots(13)$$

【００４０】

なお、上記例では、基数積D_iに乱数$\{v_i\}$を付加するようにしたが、このような乱数を付加せず、上記（３）で示される基数積D_iをそのまま用いても良い。

【００４１】

（第２実施の形態）

秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：$\{d_i^{(P)}\}$，$\{d_i^{(Q)}\}$，$\{d_i^{(P)\prime}\}$，$\{d_i^{(Q)\prime}\}$，$\{v_i^{(P)}\}$，$\{v_i^{(Q)}\}$，P，Q，N，w

・公開鍵：$\{c_i\}$

なお、上記Ｎは公開であっても良い。

【００４２】

Ｐ，Ｑを後述の条件を満たす素数とする。$e > e'$とし、正規基数$d_i^{(P)}$，$d_i^{(Q)}$及び退化基数$d_i^{(P)\prime}$，$d_i^{(Q)\prime}$は、夫々下記（14），（15）を満たす基数と定義する。

【００４３】

【数６】

$$d_i^{(P)} d_i^{(Q)} = 2^e + \delta_i \quad (1 \ll \delta_i \ll 2^e) \cdots (14)$$

$$d_i^{(P)\prime} d_i^{(Q)\prime} = 2^{e'} + \delta_i' \quad (1 \ll \delta_i' \ll 2^{e'}) \cdots (15)$$

【００４４】

法Ｐ及び法Ｑについて、夫々第１実施の形態と同様に、２組の基数$\{d_i^{(P)}\}$，$\{d_i^{(P)\prime}\}$及び$\{d_i^{(Q)}\}$，$\{d_i^{(Q)\prime}\}$を生成する。但し、任意の$i \in I''$について、下記（16），（17）を満たすものとする。

$$\gcd(d_i^{(P)}, d_i^{(Q)}) = 1 \quad \cdots (16)$$

$$\gcd(d_i^{(P)\prime}, d_i^{(Q)\prime}) = 1 \quad \cdots (17)$$

【００４５】

次に、法Ｐ及び法Ｑについて、第１実施の形態と同様に、２組の乱数$\{v_i^{(P}$

) } 及び { $v_i^{(Q)}$ } を生成し、上記（３），（４）と同様の計算により、{ $V_i^{(P)}$ } 及び { $V_i^{(Q)}$ } を導く。

【００４６】

第１実施の形態と全く同様に構成された拡大平文ベクトルｍ″に対する法Ｐ及び法Ｑにおける積和平文M_P 及び積和平文M_Q を夫々、下記（18），（19）と定義する。

$$M_P = m_1 \text{″} V_1^{(P)} + m_2 \text{″} V_2^{(P)} + \cdots + m_{K+R} \text{″} V_{K+R}^{(P)} \quad \cdots (18)$$

$$M_Q = m_1 \text{″} V_1^{(Q)} + m_2 \text{″} V_2^{(Q)} + \cdots + m_{K+R} \text{″} V_{K+R}^{(Q)} \quad \cdots (19)$$

【００４７】

更に、素数Ｐ及び素数Ｑを、任意の拡大平文ベクトルｍ″に対してM_P ＜ＰかつM_Q ＜Ｑの条件を満たすように生成し、それらの積をＮとする。中国人の剰余定理を用いて、Ｐ及びＱによる余りが夫々$V_1^{(P)}$ 及び$V_1^{(Q)}$ となるような最小の$V_1^{(N)}$ （＜Ｎ）を導いて変換基数積と定義する。

【００４８】

積和平文Ｍを，拡大平文ベクトルｍ″と変換基数積$V_1^{(N)}$ とを用いて、下記（20）のように定義する。ここで、Ｍ＜Ｎを満たす必要はない。

$$M = m_1 \text{″} V_1^{(N)} + m_2 \text{″} V_2^{(N)} + \cdots + m_{K+R} \text{″} V_{K+R}^{(N)} \quad \cdots (20)$$

【００４９】

Ｎより小さい乱数ｗを定め、下記（21）に従って、下記（22）に示すような公開鍵ベクトルｃを導いて公開する。

$$c_i \equiv w V_i \pmod N \quad \cdots (21)$$

$$\text{ベクトル} c = (c_1, c_2, \cdots, c_{K+R}) \quad \cdots (22)$$

【００５０】

エンティティａ側で、拡大平文ベクトルｍ″と公開鍵ベクトルｃとの内積を下記（23）のように求めて、暗号文Ｃを得る。作成された暗号文Ｃは通信路３を介してエンティティａからエンティティｂへ送信される。なお、Ｎを公開する場合

には、下記（23）のＣをＮで割った剰余を暗号文とすれば良い。

$$C = m_1'' c_1 + m_2'' c_2 + \cdots + m_{K+R}'' c_{K+R} \quad \cdots (23)$$

【００５１】

エンティティｂ側では、以下のようにして復号処理が行われる。

積和平文Ｍは、下記（24）を満たす。従って、法Ｐ及び法Ｑにおける積和平文M_P及びM_Qは、下記（25），（26）のようにして求めることができる。

$$M \equiv w^{-1} C \pmod{N} \quad \cdots (24)$$

$$M_P \equiv M \pmod{P} \quad \cdots (25)$$

$$M_Q \equiv M \pmod{Q} \quad \cdots (26)$$

【００５２】

拡大平文ベクトルｍ″のうち、正規基数に対応するインデックス、即ち、ｉ∈Ｉに関しては、$2^e < d_i^{(P)} d_i^{(Q)}$であるため、下記（27），（28）によって（$m_i^{(P)}$，$m_i^{(Q)}$）を求め、中国人の剰余定理を適用することにより、下記（29）が成立して、平文ベクトルｍを復号することができる。

【００５３】

【数７】

$$m_i^{(P)} \equiv M_P V_i^{(P)-1} \pmod{d_i^{(P)}} \cdots (27)$$

$$m_i^{(Q)} \equiv M_Q V_i^{(Q)-1} \pmod{d_i^{(Q)}} \cdots (28)$$

$$m_i \equiv \begin{cases} m_i^{(P)} \pmod{d_i^{(P)}} \\ m_i^{(Q)} \pmod{d_i^{(Q)}} \end{cases} \cdots (29)$$

【００５４】

なお、退化基数に対応するインデックス、即ち、ｉ∈Ｉ′に関しては、第１実施の形態と同様、復号する必要がなく、疑似平文ベクトルｍ′を正しく復号することができない。

【００５５】

なお、上記例では、２組の基数｛$d_i^{(P)}$｝，｛$d_i^{(Q)}$｝に乱数｛$v_i^{(P)}$

｝，｛$v_i^{(Q)}$｝を付加するようにしたが、このような乱数を付加しない基数積を使用しても良い。

【００５６】

次に、上述したような本発明の方式にあって、ＬＬＬアルゴリズムに基づく低密度攻撃に強い耐性を持てるように、１を超える高い密度を実現できていることを説明する。退化していない一般的な積和型暗号について、暗号文密度σ，方式密度ρ，レートηを下記（30），（31），（32）のように定義する。なお、Ｃは暗号文のビット数，C_{max}は取り得る最大の暗号文のビット数，Ｋは平文の分割数，ｅは分割平文のビット数である。

【００５７】

【数８】

$$\sigma = \frac{\sum_{i=1}^{K} \log_2 m_i}{\log_2 C} \quad \cdots (30)$$

$$\rho = \frac{Ke}{\log_2 C_{max}} \quad \cdots (31)$$

$$\eta = \frac{Ke}{|C_{max}|} \quad \cdots (32)$$

【００５８】

また、本発明のように退化している積和型暗号について、暗号文密度σ′，方式密度ρ′を下記（33），（34）のように定義する。なお、レートは上記（32）と同じである。

【００５９】

【数９】

$$\sigma' = \frac{\sum_{i=1}^{K+R} \log_2 m_i''}{\log_2 C} \quad \cdots (33)$$

$$\rho' = \frac{(K+R)e}{\log_2 C_{max}} \quad \cdots (34)$$

【００６０】

第１実施の形態における密度について考察する。乱数v_iをｓビットとする。密度をできる限り大きくするために、取り得る最大の積和平文をM_{max}とした場合、法Ｐのビットサイズを｜Ｐ｜＝｜M_{max}｜と設定すべきである。この場合、第１実施の形態における方式密度ρ_1，レートη_1は、夫々、下記（35），（36）の条件を満たす。

【００６１】

【数１０】

$$\rho_1 = \frac{(K+R)e}{e+\log_2 P+\log_2(K+R)} > \frac{(K+R)e}{(K+2)e+(R-1)e'+s+2\log_2(K+R)+1} \quad \cdots (35)$$

$$\eta_1 = \frac{Ke}{e+\log_2 P+\log_2(K+R)} > \frac{Ke}{(K+2)e+(R-1)e'+s+2\log_2(K+R)+1} \quad \cdots (36)$$

【００６２】

公開鍵より秘密鍵を求める攻撃（片柳磨子，村上恭通，笠原正雄：”積和型暗号に関する二，三の考察”，1999年暗号と情報セキュリティシンポジウム資料，Ｂ43 Jan.2000 に開示）を回避するためには、乱数v_iのビットサイズを法Ｐのビットサイズの１／４以上にする必要がある。この条件を満たすように、乱数v_iのビットサイズを$s=(1/4)\log_2 P+1$と考えて計算した場合、方式密度ρ_1，レートη_1は、夫々、下記（37），（38）の条件を満たす。

【００６３】

【数１１】

$$\rho_1 > \frac{3(K+R)e}{(4K+7)e+4(R-1)e'+7\log_2(K+R)+7} \quad \cdots (37)$$

$$\eta_1 > \frac{3Ke}{(4K+7)e+4(R-1)e'+7\log_2(K+R)+7} \quad \cdots (38)$$

【００６４】

この条件において、乱数v_iが非常に大きいので、ｅ′をｅ′＜ｅ／２とする、または、Ｋ＜Ｒとすることにより、$\rho_1>1$を満たすパラメータが存在する。

【００６５】

第２実施の形態における密度について考察する。乱数$v_i^{(P)}$と$v_i^{(Q)}$との積、即ち、$v_i^{(P)}v_i^{(Q)}$をｓビットとする。法Ｎが非公開である場合、密度をできる限り大きくするために、取り得る最大の積和平文をM_{Pmax}，M_{Qmax}としたとき、$|P|=|M_{Pmax}|$，$|Q|=|M_{Qmax}|$と設定すべきである。この場合、第２実施の形態における方式密度ρ_2，レートη_2は、夫々、下記（39），（40）の条件を満たす。

【００６６】

【数１２】

$$\rho_2 = \frac{(K+R)e}{e+\log_2 N+\log_2(K+R)}$$

$$> \frac{(K+R)e}{(K+3)e+(R-1)e'+s+3\log_2(K+R)+1} \quad \cdots (39)$$

$$\eta_2 = \frac{Ke}{e+\log_2 N+\log_2(K+R)}$$

$$> \frac{Ke}{(K+3)e+(R-1)e'+s+3\log_2(K+R)+1} \quad \cdots (40)$$

【００６７】

第２実施の形態では、多重化しているので、乱数をあまり大きくする必要はない。よって、ｅ′＝ｅ／２，Ｋ＝Ｒという条件であっても、容易に方式密度ρ_2＞１，レートη_2＞１／２を達成することができる。例えば、上記の条件において、分割数をＫ＝８とし、基数$d_i^{(P)}$，$d_i^{(Q)}$及び乱数$v_i^{(P)}$，$v_i^{(Q)}$を何れも３２ビットとした場合、ρ_2＝1.0174，η_2＝0.5087となり、このような小さなパラメータでも、上記の条件（ρ_2＞１，η_2＞１／２）を実現できている。但し、小さなパラメータでは安全性に問題があるので、例えばＫ＝１００，ｅ＝６４，ｅ′＝３２程度が現実的である。

【００６８】

また、法Ｎを公開とし、ＣをＮで割った剰余を暗号文とした場合の第２実施の形態における方式密度ρ_2，レートη_2は、夫々、下記（41），（42）の条件を満たす。

【００６９】

【数１３】

$$\rho_2 = \frac{(K+R)e}{\log_2 N}$$

$$> \frac{(K+R)e}{(K+2)e+(R-1)e'+s+2\log_2(K+R)+1} \quad \cdots (41)$$

$$\eta_2 = \frac{Ke}{\log_2 N}$$

$$> \frac{Ke}{(K+2)e+(R-1)e'+s+2\log_2(K+R)+1} \quad \cdots (42)$$

【００７０】

以上のように、法Ｎを公開とした場合には、法Ｎが非公開である場合に比べて、方式密度ρ_2，レートη_2の何れもが向上している。

【００７１】

ところで、疑似平文ベクトルｍ′における乱数成分は、平文ベクトルｍとは全く独立して設定できる。よって、作成した暗号文Ｃの方式密度が高くなるように疑似平文ベクトルｍ′の乱数成分を設定するようにすれば良い。また、疑似平文ベクトルｍ′としてある乱数系列を設定して暗号文Ｃを作成した後、その暗号文Ｃの方式密度を計算し、その計算値が１を超えない場合には、疑似平文ベクトルｍ′に設定する乱数系列を別なものにして暗号文Ｃを作成しなおすようにし、方式密度が１を超えた場合の暗号文Ｃを受信先のエンティティへ送信する手法が有効である。

【００７２】

図２は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、第１または第２実施の形態における上述した手順に従って拡大

平文ベクトルm″と公開鍵ベクトルｃとの内積計算により暗号文Ｃを作成する処理を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ10は、送信側のエンティティに設けられている。

【００７３】

図２において、コンピュータ10とオンライン接続する記録媒体11は、コンピュータ10の設置場所から隔たって設置される例えばＷＷＷ(World Wide Web)のサーバコンピュータを用いてなり、記録媒体11には前述の如きプログラム11a が記録されている。記録媒体11から読み出されたプログラム11a がコンピュータ10を制御することにより、コンピュータ10が暗号文Ｃを作成する。

【００７４】

コンピュータ10の内部に設けられた記録媒体12は、内蔵設置される例えばハードディスクドライブまたはＲＯＭなどを用いてなり、記録媒体12には前述の如きプログラム12a が記録されている。記録媒体12から読み出されたプログラム12a がコンピュータ10を制御することにより、コンピュータ10が暗号文Ｃを作成する。

【００７５】

コンピュータ10に設けられたディスクドライブ10a に装填して使用される記録媒体13は、運搬可能な例えば光磁気ディスク，ＣＤ－ＲＯＭまたはフレキシブルディスクなどを用いてなり、記録媒体13には前述の如きプログラム13a が記録されている。記録媒体13から読み出されたプログラム13a がコンピュータ10を制御することにより、コンピュータ10が暗号文Ｃを作成する。

【００７６】

【発明の効果】

以上のように、本発明では、暗号化すべき平文を分割してなる第１ベクトル（平文ベクトル）に暗号化を必要としない乱数成分からなる第２ベクトル（疑似平文ベクトル）を加えた第３ベクトル（拡大平文ベクトル）と、各成分を$D_i = d / d_i$ または$V_i = (d / d_i) \cdot v_i$ に設した第４ベクトル（基数ベクトル）とを用い、積和演算方式にて暗号文を構成するようにしたので、暗号文の密度を大きくでき、ＬＬＬアルゴリズムに基づく低密度攻撃に対して強くなって安全性

を向上できる。この結果、積和型暗号の実用化の道を開くことに、本発明は大いに寄与できる。

【図面の簡単な説明】

【図１】

２人のエンティティ間における情報の通信状態を示す模式図である。

【図２】

記録媒体の実施の形態の構成を示す図である。

【符号の説明】

１　暗号化器

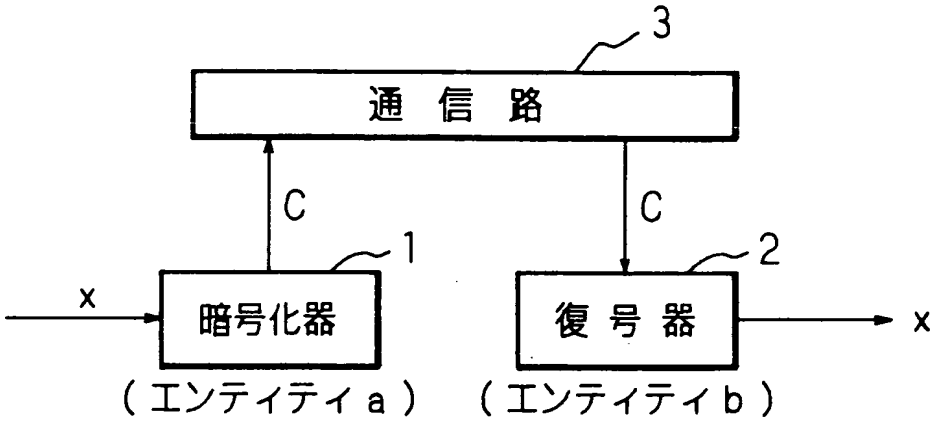
２　復号器

３　通信路

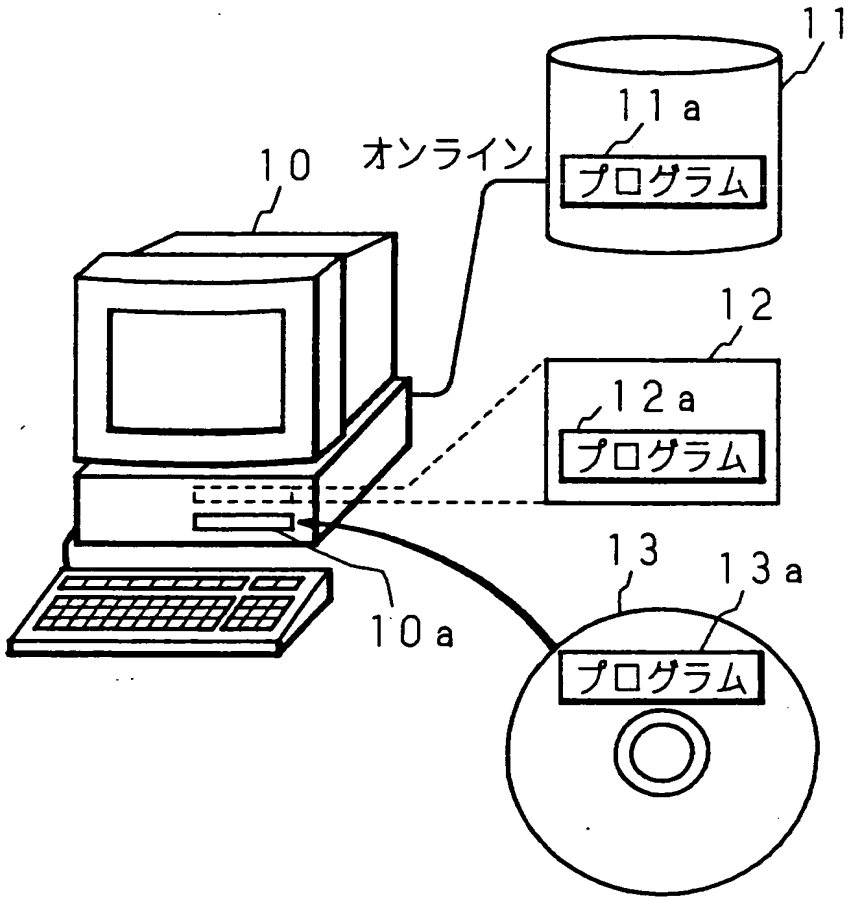
ａ，ｂ　エンティティ

【書類名】　　図面

【図１】



【図２】



【書類名】　　要約書

【要約】

【課題】　ＬＬＬアルゴリズムに基づく低密度攻撃に強く、安全性を向上できる暗号化方法を提供する。

【解決手段】　暗号化すべき平文をＫ分割した平文ベクトルｍ＝（m_1，m_2，…，m_K）に任意の乱数成分からなる疑似平文ベクトルｍ′＝（m_{K+1}'，m_{K+2}'，…，m_{K+R}'）を加えた拡大平文ベクトルｍ″＝（m_1''，m_2''，…，m_{K+R}''）と、整数d_i（$1 \leqq i \leqq K+R$）及び乱数v_iを用いて$D_i = d / d_i \cdot v_i$（但し、$d = d_1 d_2 \cdots d_{K+R}$（任意の２つの整数$d_i$，$d_j$は互いに素））に設定された基数ベクトルＤ＝（$D_1$，$D_2$，…，$D_{K+R}$）とを用いて、積和型の暗号文を得る。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－１５３３５８
受付番号	５００００６４０７４３
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１２年　５月２５日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】　000006297

【住所又は居所】　京都府京都市南区吉祥院南落合町３番地

【氏名又は名称】　村田機械株式会社

【特許出願人】

【識別番号】　597008636

【住所又は居所】　大阪府箕面市粟生外院４丁目１５番３号

【氏名又は名称】　笠原　正雄

【代理人】　申請人

【識別番号】　100078868

【住所又は居所】　大阪府大阪市中央区釣鐘町二丁目４番３号　河野特許事務所

【氏名又は名称】　河野　登夫

【選任した復代理人】

【識別番号】　100114557

【住所又は居所】　大阪府大阪市中央区釣鐘町二丁目４番３号　河野特許事務所

【氏名又は名称】　河野　英仁

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００６２９７〕

１．変更年月日　　１９９０年　８月　７日
［変更理由］　新規登録
住　所　京都府京都市南区吉祥院南落合町３番地
氏　名　村田機械株式会社

出　願　人　履　歴　情　報

識別番号　　〔５９７００８６３６〕

１．変更年月日　　１９９７年　１月２１日
［変更理由］　新規登録
住　所　　大阪府箕面市粟生外院４丁目１５番３号
氏　名　　笠原　正雄